CLAIM AMENDMENTS

This listing of claims will replace all prior versions and listings of claims in the application.

1. (Currently Amended) A method of detecting denial of service (DoS) attacks in an Internet accessible network having at least one proxy server incorporating a session initiation protocol (SIP), said SIP including incoming INVITE messages that request set-up of an Internet telephone call and outgoing 180 Ringing messages that indicate ringing, the method comprising ~~the following steps~~:

aggregating said INVITE messages and said 180 Ringing messages for all users on said Internet accessible network;

detecting an imbalance between a number of said INVITE and 180 Ringing messages resulting from a DoS attack; and

providing an indication of ~~the~~ a presence of a current DoS attack on said proxy server based on detection of said imbalance.

2. (Currently Amended) The method of claim 1,

wherein a number (H) of INVITE messages including credentials that are sent from a user client in response to an authentication required message from the proxy server, said credentials being information used by the proxy server to

authenticate the INVITE messages, are removed from ~~the~~ an accounting before the ~~balance~~ imbalance is tested such that when ~~the~~ an equation:

INV_o [[to]] + INV_c - H = N_{180}

where INV_o is ~~the~~ a number of INVITE messages without said credentials,

INV_c is ~~the~~ a number of INVITE messages with said credentials, and

N_{180} is ~~the~~ a number of said 180 Ringing messages,

is not true within a predetermined margin of error,

then the presence of ~~a~~ said current DoS attack on the proxy server is indicated by ~~the~~ an inequality in said equation.

3. (Currently Amended) The method of claim 2, further comprising ~~including the following step~~:

~~causing said proxy server to maintain~~ creating a call information table at said proxy server for determining ~~the~~ a value of H.

4. (Canceled)

5. (Currently Amended) A system for detecting denial of service (DoS) attacks against session initiation protocol elements in ~~a~~ an Internet accessible network having at least one proxy server, said system comprising:

means for aggregating ~~said incoming~~ INVITE messages and ~~said outgoing~~ 180 Ringing messages for all users on said Internet accessible network; and

means, within said proxy server, for determining if ~~the~~ a number of ~~said~~ INVITE messages including credentials (INV_c) sent to said proxy server from user clients in response to an authentication requirement exceeds a number of said 180 Ringing messages that indicates a DoS attack, said credentials being information used by the proxy server to authenticate the INVITE messages.

6. (Currently Amended) A system for detecting denial of service (DoS) attacks in an Internet accessible network having at least one proxy server incorporating a session initiation protocol (SIP), said system comprising:

means for aggregating ~~said incoming~~ INVITE messages and ~~said outgoing~~ 180 Ringing messages for all users on said Internet accessible network; and

means, within said proxy server, for detecting an imbalance between a number of said INVITE and said 180 Ringing messages, the imbalance indicating ~~the~~ a presence of a current DoS attack on said proxy server.

7. (Previously Presented) The system of claim 5, wherein said means for determining creates a call-info table for use in tracking said INVITE messages.

8. (Currently Amended) The system of claim 6, wherein said means for detecting creates a call-info table for use in tracking said INVITE messages.